UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/665,860	09/17/2003	John Alexander Bartas	P1437	8383

24739 7590 01/11/2006

CENTRAL COAST PATENT AGENCY
PO BOX 187
AROMAS, CA 95004

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/665,860	BARTAS, JOHN ALEXANDER	
	Examiner	Art Unit	
	Longbit Chai	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-55* is/are pending in the application.

4a) Of the above claim(s) *33-55* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☒ Claim(s) *33-55* are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

During a telephone conversation with Attorney Donald R. Boys on December 9, 2005, a provisional election was made without traverse to prosecute the invention of Group I: Claims 1 – 32. Affirmation of this election must be made by Applicant in replying to this Office action. Claims 33 – 55 are withdrawn from further consideration by the Examiner, 37 CFR 1.142(b), as being drawn to a non-elected invention.

Election / Restrictions

This application contains claims directed to the following patentably distinct claimed inventions. Restriction to one of the following invention is required under 35 U.S.C 121:

I. (Group 1) Claims 1 – 32 drawn to a system for providing network security by managing and manipulating formed data connections and connection attempts initiated over a data packet network, classified in class 713, subclass 154.

II. (Group 2) Claims 33 – 43 drawn to a more specific virus detection technique of an Intrusion Detection System (IDS), classified in class 726, subclass 24.

III. (Group 3) Claims 44 – 46 drawn to a more specific denial-of-service technique of an Intrusion Detection System (IDS), classified in class 726, subclass 23.

IV. (Group 4) Claims 47 – 50 drawn to a more specific protection technique for web browser downloading in an Intrusion Detection System (IDS), classified in class 726, subclass 23.

V. (Group 5) Claims 51 – 55 drawn to a more specific Domain Name Service technique of an Intrusion Detection System (IDS), classified in class 726, subclass 23.

Inventions I – V are related as combination and subcombination disclosed as usable together in a single combination. The subcombination is distinct from the combination and the subcombinations are distinct from each other if they are shown to be separately usable. The following case instants:

Invention I has utility directed to network security by managing and manipulating formed data connections and connection attempts initiated over a data packet network through traffic filtering technique.

Invention II has separate utility directed to a more specific virus detection technique of an Intrusion Detection System (IDS) that provides fast pattern search over a data network by using a virus hash signature.

Invention III has separate utility directed to a more specific denial-of-service technique of an Intrusion Detection System (IDS) based upon the detection of SYN packet and generation of RESET packet through the host and local nodes.

Invention IV has separate utility directed to a more specific protection technique for web browser downloading in an Intrusion Detection System (IDS) that stops a download of a pop-up advertisement over a data network.

Invention V has separate utility directed to a more specific Domain Name Service technique of an Intrusion Detection System (IDS) that configures a resource on a local network for access from the network by a node using Domain Name Service protocol.

Because these inventions are distinct for the reasons given above and have acquired a separate status in the art as shown by their different classification and utility restriction for examination purpose as indicated is proper.

Examiner acknowledges that Applicant has elected Group I and as such this Office action only addresses the claimed inventions of Group I: Claims 1 – 32.

Priority

1. No claim for priority has been made in this application.

The effective filing date for the subject matter defined in the pending claims in this application is 9/17/2003.

Claim Objections

2. Claim 1 is objected to because of the following informalities: "residing on the host machine" should be "residing on the system host machine". Appropriate correction is required. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claim 32 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

According to of the specification, the only embodiment of this disclosure as presented in paragraph [0203] "the fast search pattern of the present invention also expedites searching by using a bit-masking technique to diminish the size of the hash

table index" is not specific and clear enough for enablement purpose and as such one skilled in the art clearly would not know how to make and use the same claimed invention to bit-mask the index in order to reduce the overall size of the table.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraph of 35 U.S.C. 102 that forms the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1 – 10, 12, 17 – 25 and 27 are rejected under 35 U.S.C. 102(b) as being anticipated by Jacobson et al. (U.S. Patent 6044402).

As per claim 1, Jacobson teaches a system for providing network security by managing and manipulating formed data connections and connection attempts initiated over a data-packet-network between at least two nodes connected to the network comprising:

a system host machine connected to the network; a first software application residing on the host machine for detecting and monitoring the connections and connection attempts (Jacobson: Figure 1 & 8, Column 1 Line 66 – Column 2 Line 17 and Column 25 Line 8 – 18);

a data store for storing data about the connections and connection attempts (Jacobson: Figure 8 and Column 1 Line 66 – Column 2 Line 17); and

a second software application for emulating one or more end nodes of the connections or connection attempts (Jacobson: Column 2 Line 11 –Line 15 and Column 17 Line 10 – Line 67);

characterized in that the system using the detection software detects one or more pre-defined states associated with a particular formed connection or connection attempt in progress including those associated with any data content or type transferred there over and performs at least one packet generation and insertion action triggered by the detected state or states, the packet or packets emulating one or more end nodes of the connection or connection attempt to cause preemption or resolution of the detected state or states (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 17, Jacobson teaches a software application for manipulating one or more connection ends of a data network connection between two or more network nodes operating on a data-packet-network in response to detection of a pre-defined and undesirable state or states associated with the connection comprising:

a first portion thereof for detecting one or more states associated with the connection (Jacobson: Figure 8 and Column 1 Line 66 – Column 2 Line 17);

a second portion thereof for generating packets emulating packet activity of the connection (Jacobson: Column 2 Line 11 –Line 15); and

a third portion thereof for sending the emulated packet or packets to one or more parties of the connection (Jacobson: Column 18 Line 60 – Column 19 Line 22);

characterized in that the application uses a software communication stack to send one or more Transfer Control Protocol packets emulating in construction and sequence number a packet or packets sent by a sender end of the connection, the packet received by the receiver of the connection wherein the receiving end acknowledges the packet or packets as being a valid packet or packets received from the sender of the connection, the packet or packets sent causing pre-emption or resolution of the detected state or states (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 2 and 18, Jacobson teaches the data-packet-network encompasses a Local Area Network connected to the Internet network enhanced with Transfer Control Protocol over Internet Protocol and User Datagram Protocol over Internet Protocol (Jacobson: Figure 2).

As per claim 3, Jacobson teaches the system host machine is one of a desktop computer, a router, an embedded system, a laptop computer, or a server (Jacobson: Figure 4).

As per claim 4, Jacobson teaches the system host is an especially dedicated piece of hardware (Jacobson: Figure 1 / Element 108).

As per claim 5 and 22, Jacobson teaches emulation of the end nodes of the connections or connection attempts is performed by generation and insertion into a data stream of the connection or connection attempt data packets using Transfer Control Protocol over Internet Protocol, the packets emulating packets from the current sending node in the connection (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 6 and 21, Jacobson teaches the packets inserted into a connection or connection attempt are one or a combination of Transfer Control Protocol reset packets or Transfer Control Protocol FIN packets (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 7 and 24, Jacobson teaches the nodes participating in the connections or connection attempts are desktop computers, servers, embedded systems, laptop computers or a combination thereof (Jacobson: Figure 1).

As per claim 8 and 19, Jacobson teaches the data-packet-network is an Ethernet network connected to the Internet network and the first software application is an Ethernet driver set to operate in promiscuous mode (Jacobson: Column 4 Line 28).

As per claim 9, Jacobson teaches the data about the connections or connection attempts includes one, more, or a combination of sender and receiver Internet Protocol addresses; Universal Resource Locators; source and destination ports; Transfer Control

Protocol packet sequence numbers; Ethernet machine addresses; domain names; and packet header details (Jacobson: Column 1 Line 66 – Column 2 Line 17).

As per claim 10 and 23, Jacobson teaches the data store comprises segregated datasets representing one or more of banned Internet Protocol addresses; banned domain names; banned Universal Resource Locators; banned network ports; and virus signatures (Jacobson: Column 17 Line 60 – 67).

As per claim 12, Jacobson teaches certain ones of the segregated datasets are built during runtime, maintained temporarily, and searchable by one of hash table indices or binary tree indices (Jacobson: Column 17 Line 60 – 67).

As per claim 20, Jacobson teaches manipulation of connection ends is performed by generation of and insertion of data packets to one or more nodes of the connection using Transfer Control Protocol over Internet Protocol, the generated packets emulating sender packets in construction and sequence number (Jacobson: Column 19 Line 12 – 21).

As per claim 25, Jacobson teaches Transfer Control Protocol packets are generated and inserted according to pre-defined trigger events associated with existing states or knowledge of imminence thereof discovered during operation (Jacobson: Column 17 Line 16 – 65).

As per claim 27, Jacobson teaches the predefined state is banned content and resolution thereof includes inserting content including machine readable script by one or a sequence of TCP packets containing replacement content (Jacobson: Column 19 Line 12 – 21).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 11 – 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Vaidya (U.S. Patent 6279113).

As per claim 11, Jacobson does not disclose expressly the data store further includes Ethernet machine addresses associated with bitmap icons representing individual machine types.

Vaidya teaches the data store further includes Ethernet machine addresses associated with bitmap icons representing individual machine types (Vaidya: Column 7 Line 19).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vaidya within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Vaidya teaches a more effective intrusion attempts detection method by monitoring attack signatures (Vaidya: Column 1 Line 10 – 15).

As per claim 12, Jacobson does not disclose expressly certain ones of the segregated datasets are built during runtime, maintained temporarily, and searchable by one of hash table indices or binary tree indices.

Vaidya teaches certain ones of the segregated datasets are built during runtime, maintained temporarily, and searchable by one of hash table indices or binary tree indices (Vaidya: Column 5 Line 60 – 67 and Column 9 Line 5 – 8).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vaidya within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Vaidya teaches a more effective intrusion attempts detection method by monitoring attack signatures (Vaidya: Column 1 Line 10 – 15).

As per claim 13, Jacobson does not disclose expressly certain ones of the segregated datasets are uploaded into host Random Access Memory upon booting of the host system.

Vaidya teaches certain ones of the segregated datasets are uploaded into host Random Access Memory upon booting of the host system (Vaidya: Column 5 Line 66).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Vaidya within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Vaidya teaches a more effective intrusion attempts detection method by monitoring attack signatures (Vaidya: Column 1 Line 10 – 15).

6. Claims 14 – 16, 26 and 28 – 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Joiner (U.S. Patent 6742128).

As per claim 14 and 26, Jacobson does not disclose expressly including a third software application for detecting virus activity comprising: a software routine for hashing data passed over a formed data connection; and a software routine for comparing the hash data to a dataset containing virus signatures, the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures.

Joiner teaches including a third software application for detecting virus activity comprising:

a software routine for hashing data passed over a formed data connection (Joiner: Column 4 Line 48 – 53 and Column 6 Line 10 – 17); and

a software routine for comparing the hash data to a dataset containing virus signatures, the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures (Joiner: Column 4 Line 48 – 53 and Column 6 Line 10 – 17).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Joiner within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Joiner teaches a more effective intrusion attempts detection method by assessing threats in use of profiles compared with the collected network data (Joiner: Column 3 Line 24 – 29).

As per claim 15 and 30, Jacobson as modified teaches the hashing routine utilizes at least one sliding checksum window processing data and in the case of more than one, operating simultaneously on the data creating hash values to compare against hash entries in the hash index (Joiner: Column 8 Line 47 – 53).

As per claim 16, Jacobson as modified teaches upon detecting a hit for a virus signature, the second software application interrupts data stream processing of one or more end points of the connection by sending a reset packet to stop download of the detected virus (Jacobson: Column 18 Line 60 – Column 19 Line 22).

As per claim 28, Jacobson as modified teaches virus searching is supported by algorithm supporting generation and then comparison of created hash values derived

from active connection data streams to hash table entries stored in a data store and to return a hit upon obtaining a match (Joiner: Column 4 Line 48 – 53 and Column 6 Line 10 – 17).

As per claim 29, Jacobson as modified teaches the third portion thereof is integrated with a messaging client for generating automated alerts to end nodes whose connections have been manipulated (Joiner: Column 1 Line 51 – 55).

As per claim 31, Jacobson as modified teaches each checksum window processes 9 bytes of data 3-bytes at a time, each three-byte section treated as a single 24-bit number (Joiner: Column 8 Line 47 – 53: an obvious design choice).

7. Claim 14, 26 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Caronni et al. (U.S. Patent 2002/0143850).

As per claim 14 and 26, Jacobson does not disclose expressly including a third software application for detecting virus activity comprising: a software routine for hashing data passed over a formed data connection; and a software routine for comparing the hash data to a dataset containing virus signatures, the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures.

Caronni teaches including a third software application for detecting virus activity comprising:

a software routine for hashing data passed over a formed data connection (Caronni: Para [0029] Line 12 – 22); and

a software routine for comparing the hash data to a dataset containing virus signatures, the dataset searchable by hash table index, the hash entries therein derived individually from separate virus signatures (Caronni: Para [0029] Line 12 – 22).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Caronni within the system of Jacobson because (a) Jacobson teaches an intrusion detection system, and (b) Caronni teaches a more secure intrusion attempts detection method by assigning a dedicated-purpose processing system (Caronni: Para [0012] and Para [0029] Line 12 – 22).

As per claim 28, Jacobson as modified teaches virus searching is supported by algorithm supporting generation and then comparison of created hash values derived from active connection data streams to hash table entries stored in a data store and to return a hit upon obtaining a match (Caronni: Para [0012] and Para [0029] Line 12 – 22).

8. Claims 15, 16 and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Caronni et al. (U.S. Patent 2002/0143850), and in view of Teixeira (U.S. Patent 2005/0005145).

As per claim 15 and 30, Jacobson as modified does not disclose expressly the hashing routine utilizes at least one sliding checksum window processing data and in the case of more than one, operating simultaneously on the data creating hash values to compare against hash entries in the hash index.

Teixeira teaches the hashing routine utilizes at least one sliding checksum window processing data and in the case of more than one, operating simultaneously on the data creating hash values to compare against hash entries in the hash index (Teixeira: Para [0093]).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Teixeira within the system of Jacobson as modified because (a) Jacobson teaches an intrusion detection system, and (b) Teixeira teaches blocking or modifying outgoing request when sensitive information is discovered during the process (Teixeira: Para [0011]).

As per claim 16, Jacobson as modified teaches upon detecting a hit for a virus signature, the second software application interrupts data stream processing of one or more end points of the connection by sending a reset packet to stop download of the detected virus (Teixeira: Para [0011] Line 7 – 8 & Jacobson: Column 18 Line 60 – Column 19 Line 22).

9. Claim 32 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson et al. (U.S. Patent 6044402), in view of Joiner (U.S. Patent 6742128), and in view of Weaver (U.S. Patent 6574669).

As per claim 32, Jacobson as modified does not disclose expressly the hash table is sparsely populated and wherein the index thereof is bit-masked to reduce the overall size of the table and increase performance of the search.

Weaver teaches the hash table is sparsely populated and wherein the index thereof is bit-masked to reduce the overall size of the table and increase performance of the search (O'Sullivan: Figure 7C and Column 10 Line 1 – 9).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Weaver within the system of Jacobson as modified because (a) Jacobson teaches an intrusion detection processing system based on a pre-defined pattern in the network address block list, and (b) Weaver teaches a more effective hash processing system to optimize the search over a network address hash table (O'Sullivan: Para [0076] Line 10 – 16).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LBC

Longbit Chai
Examiner
Art Unit 2131

Primary Examiner
AU 2131
1/5/06